Cible de sécurité CSPN

Secure Xchange Network (Sec-XN)

SECLAB
SIEGE : 40 AVENUE THEROIGNE DE MERICOURT 34000
MONTPELLIER

CIBLE DE SECURITE SEC-XN VERSION 3.4.0

	Nom	Fonction
Écrit par :	Benoît BADRIGNANS	Directeur technique
Vérifié par :	Ludovic MAES Fabien LAVABRE	Responsable qualité Expert Cybersécurité
Approuvé par :	AMOSSYS	CESTI

Liste d'évolutions

Révision	Date	Commentaire
0.1	19 mai 2020	Première version
0.2	3 juin 2020	Intégration remarques / conseils Amossys
1.0	30 juin 2020	Version 1.0
1.1	6 novembre 2020	Prise en compte des remarques ANSSI
1.2	18 janvier 2021	Prise en compte des remarques ANSSI

CIBLE DE SECURITE SEC-XN VERSION 3.4.0

Table des matières

CIBLE DE SECURITE SEC-XN VERSION 3.4.0

1 Introduction

1.1 Objet du document

Ce document présente la cible de sécurité du dispositif « Secure Xchange Network » en version 3.4.0, conçu et commercialisé par la société Seclab, en vue de son évaluation selon le schéma CSPN promu par l'ANSSI.

Cette cible s'appuie sur les profils de protection diode moyen terme et pare-feu moyen terme [1].

1.2 Identification produit

Éditeur	SECLAB 40 avenue Théroigne de Méricourt 34000 MONTPELLIER
Lien vers l'organisation	www.seclab-security.com
Nom commercial du produit	Secure Xchange Network (Sec-XN)
Numéro de la version évaluée	V3.4.0
Catégorie du produit	Pare-feu

1.3 Glossaire

- Réseau bas : Le réseau de confiance le plus bas. Par hypothèse il est compromis par l'attaquant
- Réseau haut : Le réseau de confiance le plus haut. Par hypothèse il n'est pas compromis par l'attaquant.
- Secure Xchange Network (Sec-XN) a aussi pour autre nom DENELIS.

1.4 Références

Pour l'établissement de la présente cible de sécurité, les documents et les liens suivants ont été consultés :

- Documentation administrateur « Secure Xchange Network » pour la version 3.4.0.
- [1] :https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/
- [2] : Vulnérabilité dans la pile TCP/IP du système d'exploitation temps réel VXWorks notamment utilisé par des fabriquants d'automates industriels : https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/
- [3] : vulnérabilité dans la pile TCP/IP de la librairie Treck affectant des millions de machines et d'appareils IoT https://www.jsof-tech.com/ripple20/

2 Description

2.1 Description générale des produits Secure Xchange de Seclab

Les produits Seclab de la gamme SX disposent d'une architecture trois-tiers : deux guichets séparés par un élément d'isolation matériel (nommé « core »). Cette architecture pourrait se comparer à celle d'une diode réseau, à la différence majeure que **ces produits permettent des échanges bidirectionnels.**

Le « core » est réalisé à l'aide d'électronique programmable. Cette implémentation matérielle, dépourvue de logiciel, garantit l'isolation des deux guichets. Cette architecture assure la résilience des systèmes protégés, même en cas de compromission du guichet exposé.

De plus, pour cloisonner les systèmes auxquels ils sont connectés, ces produits appliquent une rupture protocolaire grâce à leurs proxy intégrés.

2.2 Description générale de la cible de sécurité

La cible de sécurité (Target of Security – TOE) permet la communication bidirectionnelle entre deux réseaux de niveaux de sécurité différents, tout en assurant un cloisonnement fort de ceux-ci. Ce cloisonnement est assuré par ses proxy intégrés supportant les protocoles réseaux TCP, UDP, FTP, FTPs et sFTP.

Si l'administrateur l'autorise, la TOE permet donc le transfert de fichiers (module FT – File Transfer) et/ou des protocoles réseaux basés sur TCP ou UDP (module TP – Transport Protocol).

Il est important de noter que ces modules sont activables indépendamment et qu'ils peuvent être utilisés en même temps

La TOE prend la forme d'un « rack 19 pouces », elle est composée de deux guichets qui disposent chacun :

- D'une interface réseau pour les flux métier (cuivre ou fibre)
- D'une interface réseau d'administration (cuivre)
- D'une interface locale d'administration (console)
- D'un système d'exploitation portant les proxy et l'interface d'administration

Face avant de la TOE

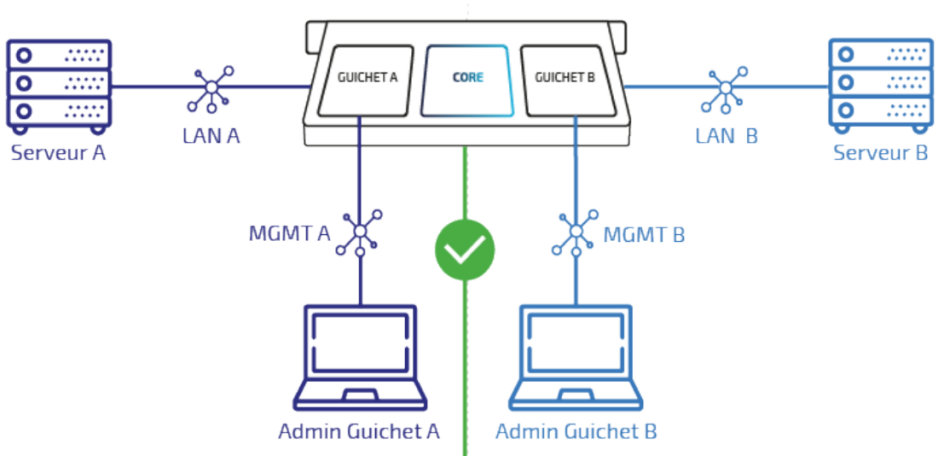
Face arrière de la TOE

En application des recommandations du guide [1] de l'ANSSI, « Secure Xchange Network (Sec-XN) » peut être utilisé pour :

- isoler des réseaux de criticités différentes (classe 1 et classe 2).
- protéger un réseau industriel connecté à un système d'information de gestion.
- cloisonner différentes parties d'un système industriel.

2.2.1 Description des fonctions de la TOE

Le schéma suivant présente la TOE dans son contexte d'utilisation courant.



TOE dans son contexte d'utilisation

L'administration des guichets est réalisée depuis deux réseaux dédiés distincts.

2.2.2 Terminaison protocolaire pour les transferts de fichiers

Dans le cadre de l'utilisation du transfert de fichier, les échanges de fichiers peuvent se faire dans le sens « guichet A vers guichet B » et « guichet B vers guichet A ». Dans les deux cas, un client FTP se connecte au serveur FTP exposé par le guichet connecté à son réseau. Une fois authentifié, il accède à l'arborescence du serveur et peut voir les fichiers envoyés ou reçus (depuis l'autre GATE si l'upload a été autorisé de l'autre côté).

Lorsqu'un client dépose un fichier dans le répertoire « to-send », il est automatiquement transféré au CORE qui vérifie qu'il répond aux règles suivantes :

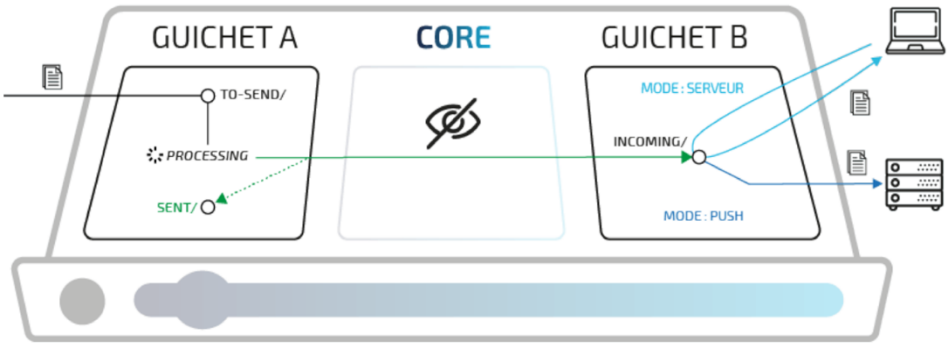
- nom encodé en UTF8-latin1 ou ASCII ;
- fichier non vide et dont la taille n'excède pas 64 Go ;
- liste blanche/noire d'extensions de fichier configurable par l'administrateur

S'il valide les contrôles, il est déplacé dans le répertoire « sent » du guichet de dépôt et transféré au guichet opposé vers le répertoire « incoming ». Le fichier est alors accessible depuis le réseau opposé. Les proxy FTP intégrés supportent les protocoles FTP, FTPs ou sFTP.

Cette rupture protocolaire permet de protéger le réseau haut face à toute attaque, même inconnues, pouvant être véhiculées par les couches de 1 à 7 (couche applicative FTP).

Par configuration, le guichet réceptionnant un fichier provenant du guichet opposé peut vérifier la signature numérique du fichier, celle-ci devant être présente sous la forme d'un autre fichier portant l'extension « .sig ». Ce mécanisme est activé pour l'évaluation.

Le schéma ci-desous représente le mécanisme pour le sens guichet A vers guichet B. Le mécanisme est similaire dans l'autre sens.



Représentation schématique pour le transfert de fichier

Par configuration, les fichiers reçus par ce mécanisme peuvent être automatiquement envoyés vers un serveur de fichier de destination (« push »). Ce mécanisme n'est pas activé pour l'évaluation.

2.2.3 Terminaison protocolaire pour les transferts de flux réseaux

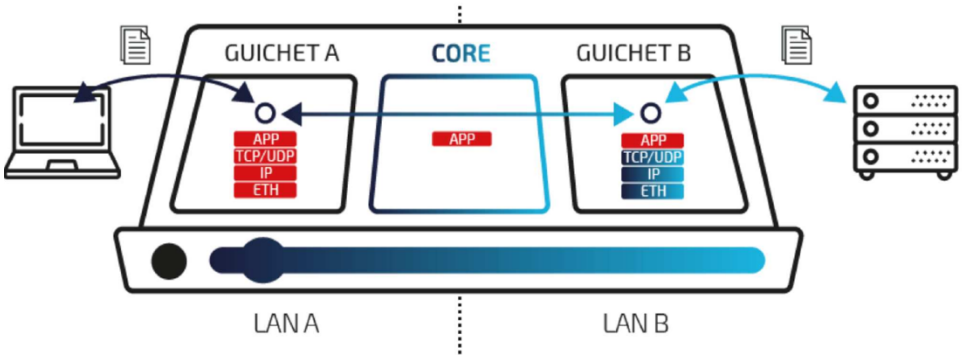
Les proxy UDP et TCP intégrés permettent de transférer des flux applicatifs d'un réseau à l'autre. Ainsi la TOE détruit les couches 1 à 4 du modèle OSI, c'est à dire :

- MAC
- IPv4
- TCP ou UDP

Ces couches **sont ensuite reconstruites** par le guichet opposé.

Cette rupture protocolaire permet de protéger le réseau haut face à toute attaque, même inconnues, pouvant être véhiculées par ces couches (voir par exemple [2, [3]).

Seule la couche application est donc transmise via le core, cette couche n'est pas filtrée par la TOE.



Représentation schématique pour le transfert de flux

2.2.4 Fonctions d'administration

Chaque guichet de la TOE est administré de manière indépendante via ses interfaces dédiées. La console d'administration de chaque guichet est accessible par un port local au format USB, et un port réseau RJ45.

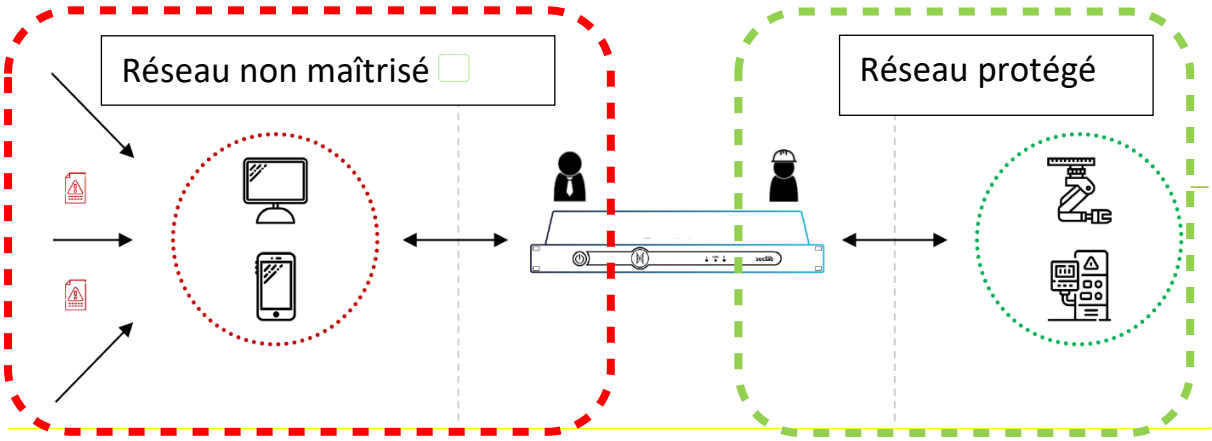
Une fois authentifié, l'administrateur peut alors configurer les services de base (ex : adresses IP des guichets, syslog, NTP,…) ainsi que les fonctionnalités de transfert apportés par les proxy UDP, TCP et/ou FTP. Il peut également procéder à :

- la mise à jour sécurisée du guichet. Celle-ci est fournie sous la forme d'un fichier « .sec » dont la signature est vérifiée ;
- la consultation des journaux. La ToE génère des journaux locaux d'évènements notamment de sécurité et d'administration. Ceux-ci sont stockés en mémoire RAM et supprimé à chaque

redémarrage. Il est possible de définir une politique de journalisation distante. Les évènements sont alors envoyés vers un serveur syslog dans un tunnel TLS.

2.2.5 Description de la manière d'utiliser le produit

Le produit est destiné à être positionné en coupure entre deux réseaux de criticité différente. Il est actif en permanence et administré en ligne de commande par un administrateur authentifié.



2.2.6 Description de l'environnement prévu pour son utilisation

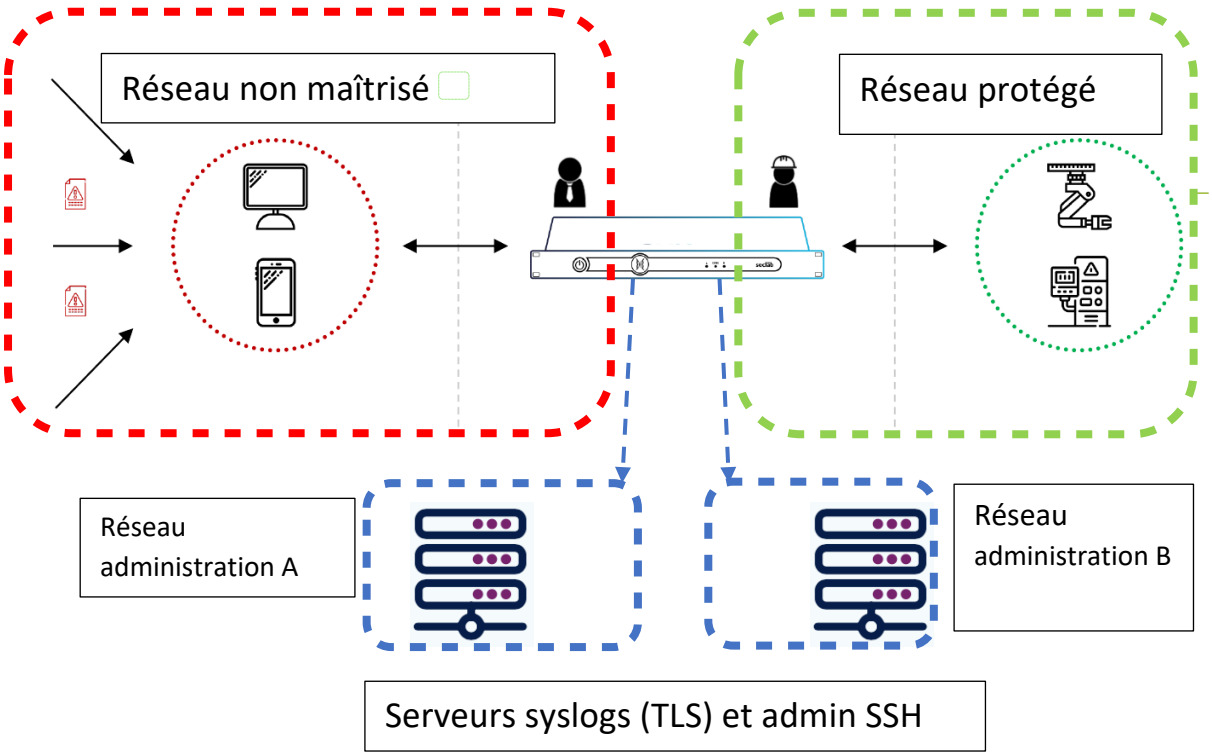
La TOE est un boitier (une appliance matérielle) embarquant son propre système d'exploitation « SecOS » basé sur la distribution Linux Debian. Elle est administrée localement ou à distance via un poste Windows, Linux ou MACOS.

2.2.7 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit

La TOE est une boîtier autonome et ne nécessite aucun autre matériel ou logiciel pour fonctionner.

2.3 Périmètre de l'évaluation

2.3.1 Plateforme d'évaluation



2.3.2 Périmètre

La TOE est le produit « Secure Xchange Network » composée des modules « File Transfer » et « Transport Protocol », positionnée en coupure entre :

- un réseau de haute confiance (LAN B) dit réseau « haut » ;
- un réseau de moindre confiance (LAN A) dit réseau « bas », susceptible de contenir un attaquant ;
- deux réseaux d'administration cloisonnés, susceptible de contenir un attaquant.

Les serveurs syslog utilisés pour le déport des journaux, présents sur les réseaux d'administration, sont hors du périmètre de l'évaluation.

La configuration et le mode d'utilisation soumis à l'évaluation sont les suivants :

- Le mot de passe par défaut de l'administrateur de chaque guichet est changé (H7).
- Les proxy FTP sont activés et configurés pour supporter uniquement le protocole FTPs.
- Le module File Transfert est configuré en mode serveur.
- Le guichet de plus haute confiance est configuré pour vérifier la signature numérique des fichiers provenant du réseau de moindre confiance. Une clef publique est générée hors de la TOE et importée par l'administrateur.

- Des canaux TCP et UDP sont activés et configurés.
- Le serveur SSH d'administration de chaque guichet est activé et dispose d'une clef SSH importée par l'administrateur.
- Les serveurs syslog de chaque guichet sont activés et configurés pour utiliser TLS.

3 Problématique de sécurité

3.1 Description des différents utilisateurs

Par définition, les utilisateurs concernent les personnes, les équipements ou des programmes tiers. Par ailleurs, une même personne physique peut être administrateur des deux guichets.

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :

- **L'administrateur du guichet A**: Utilisateur ayant les droits de modifier la configuration du guichet A de la ToE et de consulter ses journaux.
- **L'administrateur du guichet B**: Utilisateur ayant les droits de modifier la configuration du guichet B de la ToE et de consulter ses journaux.
- **L'utilisateur final** : Équipement terminal connecté directement ou indirectement à la ToE et qui échange des informations avec un réseau de criticité différente.

3.2 Description des biens sensibles à protéger

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité.

Les biens sensibles de la ToE sont les suivants :

- B1. **Firmware des guichets** : Afin d'assurer correctement ses fonctions, les firmware de la ToE doivent être intègres et authentiques.
- B2. **Configuration des guichets** : Les configurations de la ToE doivent être confidentielles et intègres. L'attaquant ne doit pas pouvoir découvrir cette configuration autrement que par l'observation de l'activité de la ToE.
- B3. **Secrets de connexion des utilisateurs** : Il s'agit des mots de passe (administrateur et FTP) et des clefs SSH. Ils sont contenus dans la ToE. Ils doivent être intègres et accessibles aux seuls utilisateurs autorisés.
- B4. **Flux de journalisation** : Les journaux déportés émis par la ToE doivent être disponibles, intègres et authentifiés.
- B5 : **Flux réseau entre les deux réseaux** : les communications entre les équipements terminaux doivent être conformes à la configuration mise en place. En particulier, les fichiers transférés vers le réseau bas doivent être protégés et authentifiés.

- B6 : **Informations du réseau protégé** : les informations du réseau protégé concernées par la rupture protocolaire. En particulier, les informations d'un guichet ne doivent pas être accessible depuis le guichet opposé.

Les besoins de sécurité pour les biens sensibles de la ToE sont les suivants :

	Disponibilité	Intégrité	confidentialité	authenticité
B1. Firmware des guichets		√		√
B2. Configuration des guichets	D	√	√	
B3. Secrets de connexion des utilisateurs	D	√	√	
B4. Flux de journalisation	D	√	√	√
B5 : Flux réseau entre les deux réseaux	D	√	√	√
B6 : Informations du réseau protégé			√	√

3.3 Description des hypothèses sur l'environnement

Les hypothèses suivantes sont formulées sur l'environnement et les conditions d'utilisation de la ToE:

- H1. **Consultation des journaux** : Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.
- H2. **Administrateurs de confiance** : Les administrateurs de la ToE sont compétents, formés et non hostiles.
- H3. **Environnement sécurisé** : La ToE est dans un local sécurisé, accessible uniquement des administrateurs. Par suite, l'administration locale n'est pas accessible par un attaquant.
- H4. **Unicité de l'interconnexion** : La TOE est le seul équipement d'interconnexion entre les deux réseaux.
- H5. **Dimensionnement** : Il est supposé que la ToE est dimensionnée correctement pour les traitements qu'elle doit effectuer.
- H6. **Services non évalués désactivés par défaut** : L'ensemble des services présents dans la ToE mais en dehors du périmètre de l'évaluation sont désactivés dans la configuration par défaut (parfois appelée configuration usine).
- H7. **Documentation de sécurité** : La ToE est fournie avec une documentation détaillée sur l'utilisation sécurisée de l'équipement. En particulier, l'ensemble des secrets de connexion présents par défaut est listé pour permettre leur personnalisation. L'ensemble des préconisations issues de cette documentation ont été appliquées en vue de l'évaluation.

- H8. **Réseau bas compromis** : On considère que le réseau bas (y compris le réseau d'administration dédié) est compromis par un attaquant. Par contre, le réseau haut (y compris le réseau d'administration dédié) est de confiance.
- H9. **Bonne compréhension du fonctionnement de la TOE** : l'administrateur est conscient que la TOE n'inspecte pas la couche applicative quand elle est utilisée pour transmettre des flux réseau. En configurant le produit et les applications du réseau protégé, il prend les mesures nécessaires pour empêcher les attaques et les fuites d'information pouvant utiliser cette couche.

3.4 Description des menaces

Par définition, une menace est une action ou un évènement susceptible de porter préjudice à la sécurité de la cible évaluée.

Les agents menaçants suivants ont été retenus :

- **Équipement terminal malveillant sur le réseau bas** : Un équipement terminal connecté à la ToE est contrôlé par l'attaquant.
- Équipement terminal malveillant sur le réseau bas **disposant des secrets d'authentification** utilisateur du proxy FTP du guichet bas.
- **Équipement d'administration malveillant sur le guichet bas** : Un équipement présent sur le réseau d'administration du guichet bas de la ToE est contrôlé par l'attaquant sans que ce dernier ne dispose nécessairement d'identifiants d'authentification valides auprès de la ToE.

Les menaces suivantes sont retenues :

- M1. **Déni de service sur le réseau haut** : L'attaquant parvient à effectuer un déni de service sur le réseau haut en effectuant une action imprévue ou en exploitant une vulnérabilité depuis le réseau bas (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu).
- M2. **Contournement de la politique de filtrage** : L'attaquant parvient à violer la politique de filtrage en permettant à un flux/fichier illégitime de transiter au travers de la ToE.
- M3. **Corruption de la politique de filtrage** : L'attaquant parvient à modifier la configuration de la TOE (afin de désactiver le transfert de fichier sécurisé par ex).
- M4. **Violation du cloisonnement** : L'attaquant arrive à accéder à un fichier du guichet haut à partir du guichet bas.
- M5. **Corruption du firmware** : L'attaquant parvient à injecter et faire exécuter un firmware corrompu sur la ToE. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée.
- M6. **Corruption d'une mise à jour** : L'attaquant parvient à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans la ToE par des moyens légitimes. L'attaquant peut également tenter d'installer une version légitime du firmware sans en avoir le droit.
- M7. **Corruption de la configuration** : L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la ToE.
- M8. **Compromission de la configuration** : L'attaquant parvient à récupérer tout ou partie de la configuration de la ToE de manière illégitime.

- M9. **Élévation de privilèges** : L'attaquant parvient à s'authentifier sans avoir les secrets de connexion, ou après les avoir dérobés.
- M10. **Corruption des flux de journalisation** : L'attaquant parvient à supprimer ou modifier un flux de journalisation distante sans que le destinataire ne puisse s'en rendre compte.

3.5 Fonctions de sécurité

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité de la TOE sont les suivantes :

- F1. **Gestion des entrées malformées** : La ToE a été développée de manière à gérer correctement les entrées malformées, en particulier en provenance des réseaux bas.
- F2. **Rupture protocolaire** : La ToE protège le réseau haut en assurant une rupture protocolaire d'après la configuration des guichets A et B. La ToE assure la conformité protocolaire des échanges à destination du réseau haut. Via cette rupture protocolaire, la ToE masque les informations provenant du réseau protégé pour les couches concernées par celle-ci :
  - Couches 1 à 4 quand les proxy TCP ou UDP sont utilisés ;
  - Couches 1 à FTP quand les proxy FTP sont utilisés.
- F3. **Cloisonnement des guichets** : La prise de contrôle du guichet ne remet pas en cause les fonctions de sécurité du guichet opposé. En particulier, la configuration d'un guichet ne peut pas être modifiée par une action malveillante sur les interfaces du guichet opposé.
- F4. **Stockage sécurisé des secrets** : Les secrets de connexion des utilisateurs sont stockés de manière sécurisée sur la ToE et la compromission d'un fichier ne permet pas de les récupérer.
- F5. **Protection de la configuration** La politique de gestion des utilisateurs ne permet pas à une personne non-autorisée de consulter ou modifier tout ou partie de la configuration de la TOE.
- F6. **Authentification sécurisée des utilisateurs** : les utilisateurs du FTP et administrateurs s'authentifient avant toute opération. Les connexions locales (console) ou distantes (SSH) ont une durée de vie limitée. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.
- F7. **Sécurité des échanges réseau** : La TOE met en œuvre divers échanges réseaux protégés en confidentialité et intégrité :
  - **L'administration distante** via SSH ;
  - La **journalisation déportée** via syslog TLS.
- F8. **Signature du firmware** : À chaque installation d'un nouveau firmware, l'intégrité et l'authenticité de celui-ci est vérifiée. L'intégrité et l'authenticité sont également vérifiées au chargement du firmware lors du démarrage de l'équipement
- F9. **Transfert de fichier sécurisé** : Les transferts de fichiers entre réseau haut et bas se font uniquement en FTPs. D'autre part, le guichet haut de la ToE permet de vérifier l'intégrité et l'authenticité des fichiers transférés depuis le réseau bas via son proxy FTP. Cette vérification est effectuée au regard d'une signature numérique (autre fichier provenant du réseau bas) et de clefs publiques renseignées par l'administrateur du guichet haut.

3.6 Matrices de couvertures

3.6.1 Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles :

	B1. Firmware des guichets	B2. Configuration des guichets	B3. Secrets de connexion des utilisateurs	B4. Flux de journalisation	B5 : Flux réseau entre les deux réseaux	B6 : Informations du réseau protégé
M1. Déni de service		D	D	D	D	
M2. Contournement de la politique de filtrage					ICA	C
M3. Corruption de la politique de filtrage		I			I	
M4. Violation du cloisonnement						C
M5. Corruption du firmware	IA					
M6. Corruption d'une mise à jour	IA					
M7. Corruption de la configuration		I				
M8. Compromission de la configuration		C				
M9. Élévation de privilèges			C			
M10. Corruption des flux de journalisation				IC		

Couverture des biens sensibles par les menaces

3.6.2 Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

CIBLE DE SECURITE SEC-XN VERSION 3.4.0

	F1. Gestion des entrées malformées	F2. Rupture protocolaire	F3. Cloisonnement des guichets	F4.Stockage sécurisé des secrets	F5. Protection de la configuration	F6. Authentification des utilisateurs	F7. Sécurité des échanges réseau	F8. Signature du firmware	F9. Transfert de fichier sécurisé
M1. Déni de service	√							√	√
M2. Contournement de la politique de filtrage		√							√
M3. Corruption de la politique de filtrage	√								
M4. Violation du cloisonnement			√						
M5. Corruption du firmware									√
M6. Corruption d'une mise à jour					√			√	
M7. Corruption de la configuration					√				
M8. Compromission de la configuration					√				
M9. Élévation de privilèges						√	√		
M10. Corruption des flux de journalisation							√		

Couverture des menaces par les fonctions de sécurité